

## REMARKS

Applicant respectfully requests reconsideration of this application. Claims 1-31 are currently pending. Claims 1, 16, and 21 have been amended. Claims 32-34 have been added. No claims have been cancelled. Therefore, claims 1-34 are now presented for examination.

### 35 U.S.C. §112 Rejection

The Examiner has rejected claim 1 under 35 U.S.C. 112, indicating that the limitation “the non-authorized mobile device” lacks sufficient antecedent basis. Claim 1 has been amended to clarify the antecedent basis by changing “a non-authorized device” to “a non-authorized mobile device”.

### 35 U.S.C. §102 Rejection

#### Stewart, et al.

The Examiner rejected claims 1-31 under 35 U.S.C. 102 (e) as being anticipated over U.S Patent 6,732,176 of Stewart, et al. (hereinafter referred to as “Stewart”).

For convenience, **claim 1** is provided here, as amended herein:

1. A method comprising:

broadcasting a synchronization signal from a wireless access point device indicating one of a plurality of modes of operation for the access point, the plurality of modes of operation including a private mode of operation for authorized devices and a public mode of operation for authorized or non-authorized devices;

broadcasting available public network services if the mode of operation is the public mode of operation;

receiving a request for establishment of a connection from a non-authorized mobile device in response to the broadcast of a synchronization signal for the public mode of operation; and

establishing a connection between the non-authorized mobile device and the access point device;

wherein establishing a connection in the private mode comprises use of a secure authentication process, and wherein establishing a connection in the public mode comprises use of a registration process.

Applicant submits that Stewart does not provide for all elements of the claim. It is submitted that Stewart does not show establishing a connection in the private mode comprising use of a secure authentication process, and wherein establishing a connection in the public mode comprising use of a registration process.

In this case, Stewart includes a system and method for enabling different access levels within a wired or wireless network system. However, the operation and structure are different, and Stewart does not address the use of different types of authentication procedures to process public and private modes of operation.

Stewart does discuss different access levels that may be presented to an access point, indicating that “[t]he access information stored on the memory medium may also include an access level which indicates the user's access rights or privilege level.”

(Stewart, col. 3, lines 17-19) However, there is no indication in Stewart that different connection processes are used to address such different access levels.

For example, Stewart provides:

Also, if the identification information is determined to not be known, the access or privilege level of the user may be set to the lowest possible level. This, for example, may allow the user to only have access to certain limited local resources, but no external access, e.g., to the Internet. Thus, for example, where the APs 120 are located in an airport, the user having a low access level, e.g., the user whose identification information is not known, may be granted access to certain local

resources, such as coffee shops, bookstores, and advertising on the local LAN at the airport, but may not be provided with Internet access. Access to local resources may be allowed since this does not require the use of external facilities and hence does not consume off-property bandwidth, and thus is relatively inexpensive to provide. Alternatively, if the identification information of a user is determined to not be known, the system may provide some form of external access, which may be billed separately by an external Internet provider, without the user being able to view or use any local network resources

(Stewart, col. 12, lines 11-29) Stewart thus mentions that multiple access levels may exist, but separate processes for the establishment of connections are not mentioned, nor is there any indication what type of connection process is used to establish the varying access level connections.

Stewart provides structures, as shown in Figures 2 and 3, in which the access points may direct mobile users to multiple different local area networks. However, the actual access processes are not shown or discussed. There is an indication in Stewart that users with different access levels may receive different types of service, but there is no indication how these differing users are connected.

It is submitted that the arguments presented above also apply to independent **claims 16 and 21**, which contain related provisions, and for this reason, among others, these claims are not anticipated by Stewart. The remaining rejected claims are dependent claims and are allowable because they are dependent on the allowable base claims.

Specifically with regard to the elements presented in new **claims 32-34**, Stewart mentions in numerous locations that an IEEE 802.11 structure processes may be utilized, but there is no indication how the processes in Stewart would actually operate under such standards. For example:

Each wireless access point (AP) 120 may have a wireless connection or transceiver (e.g., an antenna) and may operate according to various wireless standards, such as wireless Ethernet (IEEE 802.11). ...

(Stewart, col. 5, lines 8-11)

The network 130 may also be a wireless network based on IEEE 802.11. ...

(Stewart, col. 5, lines 20-21)

In step 204 the personal computing device (PCD) 110 of the user transmits identification information (ID information) to an access point (AP) 120 of the network. The identification information may take any of various forms. In one embodiment, the identification information comprises a System ID (SID) according to IEEE 802.11. As discussed above, IEEE 802.11 (wireless Ethernet) is designed to support multiple overlapping wireless LANs in a given coverage area. IEEE 802.11 uses the System ID (SID) to "select" which LAN to use, and thus which access point with which to associate. In this embodiment each System ID may be uniquely associated with a respective network provider, and thus the user may configure the System ID on his/her PCD 110 to uniquely identify the network provider to which the user has selected or subscribed.

(Stewart, col. 10, lines 38-52)

Again, there is no indication in these provisions how the connections will be rendered and what processes are needed for public and private connections under the IEEE standards. Stewart merely mentions that components may fall under the IEEE 802.11 or other standards, without any mention of how connections might be made for differing types of modes of operation, such as a private mode of operation and a public mode of operation.

### **Conclusion**

Applicant respectfully submits that the rejections have been overcome by the amendment and remark, and that the claims as amended are now in condition for allowance. Accordingly, Applicant respectfully requests the rejections be withdrawn and the claims as amended be allowed.

### **Invitation for a Telephone Interview**

The Examiner is requested to call the undersigned at (503) 439-8778 if there remains any issue with allowance of the case.

### **Request for an Extension of Time**

The Applicant respectfully petitions for a one-month extension of time to respond to the outstanding Office Action pursuant to 37 C.F.R. § 1.136(a). A check for the necessary fee under 37 C.F.R. § 1.17 for such an extension is enclosed.

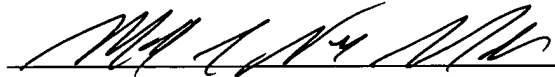
### **Charge our Deposit Account**

Please charge any shortage to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: 3/2/06

  
\_\_\_\_\_  
Mark C. Van Ness  
Reg. No. 39,865

12400 Wilshire Boulevard  
7<sup>th</sup> Floor  
Los Angeles, California 90025-1026  
(503) 439-8778